**UDK 004.056**

***Əliyev E.A.***
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
elchinaa@gmail.com

# KORPORATİV İNFORMASİYA SİSTEMLƏRİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MENECMENTİ ÜÇÜN TƏHLÜKƏSİZLİK TƏLƏBLƏRİNİN TƏSNİFAT MODELİ

*Tədqiqat işində korporativ informasiya sistemlərində informasiya təhlükəsizliyinin idarə edilməsi üçün informasiya təhlükəsizliyi tələblərinin sistemli müəyyənləşdirilməsi məqsədi ilə təsnifat modeli işlənilmişdir. Modelin təməl yaradan elementləri - təhlükəsizlik tələblərinin hədəfləri kimi informasiya sisteminə aid olan obyektlər, proseslər və subyektlər ("insan faktoru") qəbul edilir və onlar üçün təsnifat modeli təklif edilir, təhlükəsizlik tələblərinin, bu tələblərlə bağlı olan mümkün risklərin, bu risklərə adekvat olan əks-vasitələrin təsnifatlarının uzlaşdırılması və birləşmiş reyestrin yaradılması üçün ümumi platforma müəyyən edilir.*

***Açar sözlər:*** *informasiya təhlükəsizliyinin menecmenti, təhlükəsizlik tələbləri, təhlükəsizlik tələblərinin təsnifatı, təhlükəsizlik tələbinin hədəfi, adekvat mühafizə, təsnifatların uzlaşdırılması, birləşmiş reyestr.*

## Giriş

İnformasiya cəmiyyətinin inkişafi milli informasiya məkanının təhlükəsizlik sisteminin formalaşdırılmasını zəruri edir. İnformasiya təhlükəsizliyi sisteminin təyinatı – milli informasiya məkanında və onun korporativ mühitlərində informasiya təhlükəsizliyinin təmin və idarə edilməsidir [1].

Məlumdur ki, təhlükəsizlik – keyfiyyət anlayışıdır. Keyfiyyəti qiymətləndirmək üçün müvafiq meyarlardan istifadə olunur, əvvəlcədən qəbul edilmiş normativ tələblərə uyğunluq müəyyən edilir. İnformasiya təhlükəsizliyinin əsas məqsədi – informasiyanın həyat tsikli proseslərində (yaradılmasında, daşıyıcıya yazılmasında, toplanıb saxlanılmasında, emal olunmasında, istifadəsində və ötürülməsində, arxivləşdirilməsində, məhv edilməsində və s.) onun tamlıq, əlyetərlilik və konfidensiallıq xassələrinin tarazlaşdırılmış təmin edilməsidir.

İnformasiyanın həyat tsikli prosesləri müəyyən informasiya sistemində (onun arxitektur obyektləri, bu obyektlərlə bağlı olan biznes proseslər, bu proseslərin icraçıları vasitəsi ilə və ya iştirakı ilə) yerinə yetirilir, həmin sistemdə informasiya təhlükəsizliyinin adekvat təmin olunmasını, bunun üçün isə aktual təhlükəsizlik tələblərinin müəyyən olunmasını zəruri edir [2].

Bu tədqiqat işinin məqsədləri aşagıdakılardır:

a) korporativ informasiya sistemlərində konfidensial məlumatların təhlükəsizliyinin təmin olunmasına aid tələbləri sistemli müəyyənetmə və təsnifatlaşdırma modelini işləmək;
b) informasiya sistemlərinin təhlükəsizliyinin idarə edilməsi işlərinin təşkili üçün bu tələblərin hədəflərini müəyyən etmək və təsnifatlaşdırmaq;
c) informasiya sistemlərinin təhlükəsizlik parametrləri (tələbləri) üzrə monitorinqinin həyata keçirilməsini təmin etmək üçün lazım olan reyestrləri müəyyən etmək.

## Təhlükəsizlik tələblərinin təyinatı

Təhlükəsizlik tələbləri aşağıdakı prinsipləri təmin etmək üçün müəyyən edilir:

a) təhlükəsizlik hədəfinin "açıq" (mühafizəsiz) vəziyyətə keçməsinə yol verilməməsi;
b) mühafizə vasitələrini aşmağın mümkünsüzlüyünə zəmin yaradılması;
c) mühafizənin coxeşalonlu qurulması;
d) mühafizə üçün müxtəlif xarakterli vasitələrin tətbiqi;
e) səlahiyyətlərin bölüşdürülməsi və minimallaşdırılması;

f) təhlükəsizlik hədəflərinin strukturlaşması və sadə idarə olunması (“parçala – idarə et”).

Təhlükəsizlik tələbləri informasiya təhlükəsizliyinin idarə edilməsi sisteminin, bu sistem isə həmin tələblərin aid olduğu informasiya sisteminin həyat tsiklinin tərkib hissəsidir.

İnformasiya təhlükəsizliyini idarəetmə sistemi bu sahə üzrə standartın (*ISO/IEC-27001:2013*) aşağıda göstərilən tələblərini təmin etmək üçün yaradılır [3]:

a) təhlükəsizlik hadisələrinin baş verə bilmə hallarının qabaqlanması və ya azaldılması;
b) cəhd edilən və baş verən təhlükəsizlik hadisələrinin və onların subyektlərinin tez müəyyən edilməsi;
c) təhlükəsizlik insidentlərinə cavab reaksiyasının verilməsi, o cümlədən onların təsirinin daraldılması və təhlükəsizlik rejiminin bərpası;
d) təhlükəsizlik hadisələrinin operativ qeydiyyatının təmin edilməsi;
e) təhlükəsizlik insidentlərinin səbəblərinin təhlilinə imkan yaradılması.

İnformasiya sistemində təhlükəsizlik tələblərinin hədəfləri aşağıdakılardır:

a) informasiya sisteminin arxitektur obyektləri;
b) informasiya sisteminin həyat tsikli prosesləri;
c) informasiya sisteminin həyat tsikli proseslərinin icraçıları (“insan faktoru”) [4];
d) informasiya sistemi üçün istifadə edilən, onunla əlaqəsi olan digər obyekt və proseslər.

Hər bir informasiya sistemi informasiya resurslarının mühafizə qriflərindən; informasiya sistemlərinin arxitekturasının məkan üzrə paylanmış, mərkəzləşmiş və lokal olmasından; İnternetə və ya digər qlobal şəbəkələrə qoşulub-qoşulmamasından asılı olaraq müəyyən kateqoriyaya aid edilir.

Təhlükəsizlik tələblərində konfidensial məlumatların aşağıda göstərilən mühafizə qriflərinə uyğun növlü məlumatlar haqqında qanunvericiliyin müddəaları nəzərə alınır:

a) fərdi məlumat:
   - sensitiv (xüsusi) fərdi məlumat;
   - konfidensial fərdi məlumat;
b) istintaq və ya məhkəmə sirri olan məlumat;
c) bank sirri olan məlumat;
d) kommersiya sirri olan məlumat;
e) xidməti istifadə üçün məlumat;
f) peşə (həkim, notarial, vəkil və s.) sirri olan məlumat;
g) poçt-rabitə sirri olan məlumat;
h) tədqiqat və yaradıcılıq sirri olan məlumat.

Təhlükəsizlik tələbləri informasiya sistemlərinin yerləşmə məkanı və arxitekturasının mürəkkəblik dərəcəsini və aşağıdakı amilləri nəzərə alır:

1) yerləşmə məkanının ölkə daxilində olmasını:
   a) e-dövlətin informasiya sistemi, digər idarələrarası informasiya sistemləri;
   b) məkanca paylanmış korporativ informasiya sistemləri;
   c) mərkəzləşmiş korporativ informasiya sistemləri;
   d) kompüterləşmiş iş yerləri.
2) yerləşmə məkanının ölkə xaricində olmasını:
   a) ölkənin xaricdəki diplomatik və digər nümayəndəliklərində olan kompüterləşmiş iş yerləri;
   b) ölkəninin xaricinə səfərlər edən hava və dəniz nəqliyyatı vasitələrində olan bortdaxili kompüterləşmiş iş yerləri.
3) informasiya sistemlərinin (kompüterləşmiş iş yerlərinin) İnternetə və ya digər qlobal informasiya şəbəkəsinə qoşulub-qoşulmaması halını.

İnformasiya təhlükəsizliyini idarə edilməsi *ISO/IEC-27001:2013* standartına müvafiq olaraq dörd tsiklik mərhələdən ibarətdir: 1) planlaşdırma-layihələndirmə; 2) işləyib hazırlama; 3) tətbiq və nəzarət; 4) inkişaf.

İnformasiya təhlükəsizliyinin idarə edilməsinin planlaşdırma-layihələndirmə prosesləri aşağıdakı ardıcıllıqla həyata keçirilir (hədəflər – tələblər – risklər – mühafizə):

a) informasiya sistemində təhlükəsizlik tələblərinin hədəflərinin (obyektlərin, proseslərin və onların icraçılarının) dəqiqləşdirilməsi;
b) hədəf obyektləri, prosesləri və bu proseslərin icraçıları üçün təhlükəsizlik tələblərinin müəyyən edilməsi;
c) təhlükəsizlik tələbləri ilə bağlı olan mümkün risklərin, o cümlədən "təhdid pəncərələri"nin müəyyən edilməsi və qiymətləndirilməsi [5];
d) risklərə adekvat olan əks-vasitələrin müəyyən edilməsi və seçilməsi;
e) "İnformasiya təhlükəsizliyi siyasəti"nin və digər rəhbər sənədlərin hazırlanması.

**Təhlükəsizlik tələblərinin hədəfləri**

Təhlükəsizlik tələblərinin hədəfi olan obyektlərə, o cümlədən bu obyektlərin struktur (konfiqurasiya) vahidlərinə (istifadəçilərin səlahiyyət bölgüsündə iştirak edən komponentlərə) onları bir-birindən fərqləndirən identifikasiya nömrələri verilir.

Təhlükəsizlik tələblərini sistemli şəkildə müəyyən etmək üçün bu hədəflər aşağıdakı sahələr üzrə təsnifatlaşdırılır:

a) proqram təminatı vasitələri və səlahiyyətlər;
b) informasiya resursları;
c) texniki təminat vasitələri;
d) mühəndis qurğuları.

Proqram təminatı vasitələri üçün təhlükəsizlik tələbləri bu vasitələrin aşağıda göstərilən təyinat kateqoriyaları və struktur vahidləri üzrə (proqram modullarından, proqram interfeysi rejimlərindən və s.) müəyyən edilir:

a) informasiya sisteminin proqram təminatı vasitələri;
b) nəzərdə tutulan aktorlar və funksional imkanlar (səlahiyyətlər);
c) informasiya sisteminin serverində və işçi yerlərində olan əməliyyat sistemləri və məlumat bazalarını idarəetmə sistemləri;
d) informasiya sisteminin tərkib hissəsi olmayan və bu sistem üçün tətbiq edilən proqram əlavələri (vasitələri).

Proqram təminatı vasitələrinin yalnız elə imkanlarının instalyasiyası mümkün hesab edilir (aktivləşdirilir) ki, onların:

– funksionallığı məlum olsun;
– informasiya sisteminin istismarı üçün lazım olması göstərilsin;
– sınanmış olması bildirilsin.

İnformasiya resursları üçün təhlükəsizlik tələbləri aşağıda göstərilən təyinat kateqoriyaları, struktur vahidləri (məsələn, məlumat bazaları, onların məlumat cədvəlləri) və mühafizə dərəcələri (qrifləri) üzrə müəyyən edilir:

a) informasiya sisteminin təyinatı üzrə yaradılan sənədli informasiya barədə məlumat bazaları;
b) informasiya sisteminin funksionallığını təmin edən xidməti məlumat bazaları, o cümlədən "səlahiyyətlər bölgüsü matrisası", audit jurnalları, sözlüklər (lüğətlər, kataloqlar);
c) informasiya sistemində nəzərdə tutulmuş informasiya xidmətləri ilə əlaqədar edilən müraciətlər (ərizələr, sorğular) barədə məlumat bazaları.

Texniki təminat vasitələri üçün təhlükəsizlik tələbləri aşagıda göstərilən kateqoriyalar üzrə müəyyən edilir:

a) server avadanlıqları:
   - məlumat bazaları serveri;
   - proqram təminatı serveri;
   - sorğular, e-sənədlər və digər müraciətlər serveri;
   - audit jurnalları və xidməti qeydlər serveri;
   - arxiv serveri;
   - ehtiyat surətlər serveri.
b) stasionar kompüterlər, mobil terminallar (kompüterlər);
c) skanerlər, şəbəkə printerləri;
d) kompüter şəbəkəsi avadanlıqları, simli və simsiz rabitə xətləri, şəbəkələrarası şlüzlər;
e) informasiya daşıyıcıları, onlara aid konteynerlər.

Qeyd: İnformasiya sisteminin texniki təminatının struktur vahidlərinin təsnifatlı siyahısında hər bir vahidin sistemin proqram təminatının hansı struktur vahidinə əlyetərli olması işarə edilməlidir.

Mühəndis qurğuları üçün təhlükəsizlik tələbləri aşagıda göstərilən sahələr üzrə müəyyən edilir:

a) fiziki mühafizə infrastrukturu:
   - konsentrik və çoxeşalonlu "təhlükəsizlik perimetrləri" – ərazi, bina, otaq, sənəd fondları və server qovşaqları, sistem istifadəçilərinin iş yerləri üçün "giriş-çıxış" sistemləri, "icazəli dəhlizlər";
   - yanğından, elektromaqnit şüalanmasından, vibrasiyadan və digər texnogen təsirlərdən mühafizə vasitələri;
   - xəbərdarlıq vasitələri;
   - riskli sahələrdən insanları, texniki təminat vasitələrini və mühəndis qurğularını, informasiya daşıyıcılarını evakuasiya vasitələri;
   - əks-tədbir ssenariləri.
b) elektrik enerjisi infrastrukturu:
   - əsas və alternativ mənbələr;
   - fasiləsiz elektrik enerjisi ilə təchizetmə qurğuları;
   - ehtiyat elektrik generatorları.
c) telekommunikasiya infrastrukturu:
   - simli əsas və simsiz ehtiyat rabitə xətləri;
   - rabitə xətləri üçün fasiləsiz monitorinq vasitələri.
d) təchizat-təminat infrastrukturu:
   - anbarlar, konteynerlər, nəqliyyat vasitələri, qablaşdırma avadanlıqları;
   - diaqnostika, təmir-bərpa və utilizasiya alətləri;
   - kommunal təminat vasitələri, o cümlədən kondisioner sistemləri, təmizləyici avadanlıqlar, tullantı qutuları, su xətləri və tutumları.

**Təhlükəsizlik tələblərinin hədəfi olan proseslər**

İnformasiya sisteminin (komponentinin) həyat tsikli prosesləri və onların iş vahidləri olan hərəkətlər (əməliyyatlar) – təhlükəsizlik tələblərinin hədəfləridir. Bu hədəfləri sistemli şəkildə müəyyən etmək üçün aşağıda göstərilən istiqamətlər üzrə təsnifatlandırma aparılır, onlara identifikasiya nömrələri verilir:

a) planlaşdırma-layihələndirmə mərhələsi üzrə;
b) işləyib hazırlama mərhələsi üzrə;
c) tətbiq və nəzarət mərhələsi üzrə;
d) inkişaf mərhələsi üzrə.

İnformasiya sisteminin həyat tsiklinin planlaşdırma-layihələndirmə mərhələsində onun digər mərhələlərinə aid proseslər və onlar üçün təhlükəsizlik tələbləri müəyyən edilir. Bu mərhələyə aşağıdakılar aiddir:

a) informasiya sisteminə aid texniki şərtlərin (tapşırığın) hazırlanması:
   - sistemin arxitekturasına dair ilkin tələblər;
   - sistemin funksionallığına dair ilkin tələblər;
   - sistemin həyat tsikli üçün maliyyə və digər resurs hədlərinin (limitlərinin) müəyyənləşdirilməsi;
   - sistemin həyat tsikli icraçılarının kvalifikasiyasına dair ilkin tələblər;
   - sistemin arxitektur obyektlərinə, həyat tsikli proseslərinə və onların icraçılarına dair ilkin təhlükəsizlik tələbləri.
b) informasiya sisteminin layihələndirilməsi:
   - sistemin arxitektur obyektlərinin təsviri və onlar arasında dəqiqləşdirilmiş funksionallıq sxemi;
   - sistemin proqram komponentlərinin (modullarının) təyinatı, alqoritmlərin sxem və diaqramları;
   - sistemin texniki komponentlərinin (vasitələrinin) ilkin spesifikasiyası;
   - məlumat bazalarının strukturlarının layihəsi;
   - şəbəkə topologiyasının detallı layihəsi və avadanlıqlarının spesifikasiyası;
   - istifadəçi interfeyslərinin təyinatı və vizual təsviri;
   - informasiya təhlükəsizliyi siyasətinin layihəsi;
   - istismar təlimatlarının tezisləri;
   - instalyasiya və inteqrasiya işlərinə dair ümumi tələblər;
   - test sınaqları üçün plan-ssenari layihəsi;
   - razılaşdırma və ekspertiza sxeminin layihəsi.
c) informasiya sisteminin layihə sənədinin dövlət ekspertizası:
   - mülkiyyətçi (sifarişçi) tərəfindən rəsmiləşdirilmiş layihə sənədlərinə dair təhlükəsizlik tələblərinin daxiledilmə və nəzərəalınma vəziyyəti;
   - həmin təhlükəsizlik tələblərinin normativ hüquqi və texniki aktların, o cümlədən bu sənədin müddəalarına uyğun olma vəziyyəti.

İnformasiya sisteminin (komponentinin) həyat tsiklinin işləyib hazırlama mərhələsində həmin sistemin yaradılması (təkmilləşdirilməsi, inkişafı) – bu sistemin layihə sənədində göstərilmiş obyektlərin və bu obyektlərlə bağlı olan proseslərin, o cümlədən, mühafizə vasitələrinin yaradılması, layihədə nəzərdə tutulan resurslar limitinə əməl olunması təmin edilməsini nəzərdə tutur. Bu mərhələyə aşağıdakılar aiddir:

a) informasiya sistemi üçün təchizat işləri (“tədarükçü-istehsalçı-istifadəçi” zənciri):
   - tələbatın və spesifikasiyanın dəqiqləşdirilməsi;
   - tədarükçünün seçilməsi və satınalma;
   - daşıma (nəqliyyat);
   - anbara qəbul və saxlama;
   - təyinat (istifadə) yerinə təhvil.
b) informasiya sisteminin təminat (o cümlədən mühafizə) vasitələrinin yaradılması:
   - proqram və texniki modulların yaradılması və istehsalçı testləşdirilməsi;
   - komponentlərin yığılması (modulların montajı) və istehsalçı testləşdirilməsi;
   - sistemin yığılması (komponentlərin montajı) və istehsalçı testləşdirilməsi.
c) informasiya sisteminin təminat vasitələrinin quraşdırılması (montajı):
   - texniki vasitələrin montajı, proqram vasitələrinin inisalyasiya edilməsi;
   - sistemin yeni yaradılmış (təkmilləşdirilmiş) komponentinin həmin sistemə inteqrasiyası;
   - informasiya sistemi üzrə təlimlər:

- informasiya təhlükəsizliyinin əsaslarına aid seminar;
- menecment üzrə beynəlxalq sertifikatlı təlim;
- informasiya təhlükəsizliyi üzrə beynəlxalq sertifikatlı təlim;
- informasiya təhlükəsizliyi üzrə beynəlxalq standartlara aid kurslar;
- informasiya sisteminin həyat tsiklində icra etdiyi proseslərə müvafiq olan beynəlxalq sertifikatlı təlim.

d) informasiya sisteminin təhvil-təslimi:
- informasiya sisteminin layihə əsasında uyğunluq üzrə sertifikatlaşdırılması;
- informasiya sisteminin təhlükəsizlik tələblərinə uyğunluğunun yoxlanılması.

İnformasiya sisteminin (komponentinin) həyat tsiklinin tətbiq və nəzarət mərhələsi aşağıdakı prosesləri əhatə edir:

a) informasiya sisteminin istismarı, o cümlədən e-xidmətlər;
- informasiyanın yaradılması;
- informasiya-sorğu;
- informasiya-axtarış və təhlil;
- informasiya proseslərinin idarə edilməsi.

b) informasiya sisteminə texniki dəstək və yeniləmə;
- texniki dəstək və yeniləmə nəzərdə tutulan sahələrin dəqiqləşdirilməsi (sistemin (komponentin) pasportlaşdırılması);
- texniki dəstək üçün plan-qrafik və icra ssenariləri, o cümlədən icraçıların məsuliyyət bölgüsü, "24/7" rejimi;
- texniki dəstək obyektlərinin, o cümlədən mühafizə vasitələrinin funksionallıq və təhlükəsizlik vəziyyətinin profilaktika məqsədilə plan üzrə müntəzəm yoxlanılması;
- texniki dəstək obyektlərinə (əgər layihədə nəzərdə tutulubsa) məsafədən dəstək və ezamiyyət mexanizmləri;
- sistemin istismar müddəti bitmiş, mənəvi köhnəlmiş və təmiri qeyri-mümkün nasaz olan obyektlərin, layihə şərtlərindən asılı olaraq müntəzəm seçilməsi və təzələnməsi;
- təmir-bərpa işləri;
- utilizasiya işləri;
- təchizat işləri;
- texniki dəstək və təzələmə işlərinin qeydiyyatının aparılması ("help-desk" üçün müraciətlər, texniki diaqnostika rəyləri, sərf edilən materialların və ehtiyat hissələrin uçotu, işlərin cari və ümumiləşmiş aktları və hesabatları).

c) informasiya sisteminin müşayiəti və təkmilləşdirilməsi;
- müşayiət prosedurları, aşkar olunan uyğunsuzluqların və həllərin qeydiyyatı;
- uyğunsuzluqlar barədə müraciətlərin qəbulu, sistemin sınaq versiyasında situasiyanın dəqiqləşdirilməsi, təhlili, adekvat düzəlişlərin hazırlanması;
- uyğunsuzluqların aradan qaldırılması, testləşdirmə, təkmilləşdirmə və sazlama işləri;
- yeni versiyanın sertifikatlaşdırılması və təhvili;
- yeni versiyanın istismara qəbuluna dair planın hazılanması və istifadəçilərin məlumatlandırılması, mövcud və yeni versiyaların planda göstərilən müddətdə paralel istismarının təşkili, nəticələrin təhlili;
- mövcud versiyanı (yeni versiyanın istismarının nəticələrinin təhlilindən asılı olaraq) istismardan çıxartma planının hazırlanması və istifadəçilərin məlumatlandırılması, planın icrası, əvvəlki versiyada olan informasiya resurslarının mühafizəsi və auditi məqəsdilə müvafiq səlahiyyətlər üçün əlyetərliliyin təmin edilməsi.

d) informasiya sisteminin idarə olunması:
   - təhlükəsizliyin administratorluğu;
   - şəbəkənin administratorluğu;
   - məlumat bazalarının administratorluğu;
   - sistemin administratorluğu;
   - administratorluq işlərinin (insidentlər və həllərin) qeydiyyatı.

İnformasiya sisteminin inkişaf etdirilməsi yeni sistemin yaradılması qaydasına uyğun olaraq aparılır. Bu mərhələyə aşağıdakılar aiddir:

a) inkişaf barədə müraciətlərin və tələbatın təhlili;
b) informasiya sisteminin inkişafına aid təkliflərin hazırlanması.

**Təhlükəsizlik tələblərinin hədəfi olan icraçılar**

İnformasiya sisteminin (komponentinin) həyat tsikli proseslərinin qurulmasını və həyata keçirilməsini təmin edən (və ya nəzərdə tutulan) struktur vahidlərinin (struktur bölmələrinin, vəzifələrin) siyahısı aşağıda göstərilən kateqoriyalar üzrə təsnifatlaşdırılır, onlara identifikasiya nömrələri verilir:

a) informasiya sisteminin mülkiyyətçiləri (o cümlədən onların bu sistemin həyat tsikli mərhələlərinin icrasına məsul struktur bölmələr);
b) informasiya sisteminin həyat tsikli mərhələlərinin icrası həvalə edilmiş qurumlar;
c) informasiya sistemi ilə əlaqədar yaradılan tender komissiyaları;
d) informasiya sisteminin təhlükəsizliyinə nəzarət orqanı (o cümlədən onların akkreditə olunmuş konsaltinq, ekspertiza və sınaq mərkəzləri).

İnformasiya sisteminin həyat tsikli proseslərinin icraçıları olan mütəxəssis və işçilər üçün təhlükəsizlik tələbləri icra olunan bu proseslərin hər birinə olan təhlükəsizlik tələbləri əsasında və aşağıda göstərilən vəzifə kateqoriyaları üzrə müəyyən edilir:

a) informasiya sisteminin mülkiyyətçisinin məsul (sistemin həyat tsikli prosesləri üçün müvafiq maliyyə sənədlərini imzalamaq səlahiyyəti olan) rəhbər işçisi;
b) informasiya sisteminin həyat tsikli mərhələsinə (mərhələlərinə) məsul (müvafiq proseslər üçün menecment sənədlərini imzalamaq səlahiyyəti olan) rəhbər işçilər;
c) informasiya sistemi ilə əlaqədar yaradılan tender komissiyalarının (həmin sistemin mülkiyyətçisini və müvafiq dövlət təşkilatlarını təmsil edən) üzvləri;
d) informasiya sisteminin təhlükəsizliyinə nəzarət proseslərinə cəlb olunan mütəxəssislər;
e) informasiya sisteminin təhlükəsizliyinə məsul struktur bölməsinin və ya ixtisaslaşmış qurumun rəhbəri;
f) informasiya sisteminin həyat tsikli üzrə (informasiya təhlükəsizliyi proseslərini istisna etməklə) proseslərin icraçısı – operatoru təyin edilmiş struktur bölmə və ya qurumunun (qurumlarının) rəhbəri;
g) informasiya sisteminin informasiya təhlükəsizliyi proseslərinin icraçısı olan səlahiyyətli mütəxəssislər;
h) informasiya sisteminin həyat tsikli üzrə proseslərin icraçısı olan səlahiyyətli mütəxəssislər və işçilər.

Mütəxəssis və işçilər üçün təhlükəsizlik tələbləri, aşağıda göstərilən fəaliyyət istiqamətlərindən (vəzifələrindən) asılı olaraq, onların məsul təyin olunduğu sahələr (obyekt və proseslər) üzrə müəyyən edilir:

- sistemi layihələndirmə;
- sənədləşdirmə və menecment;
- proqramlaşdırma və kompüter mühəndisliyi;
- maddi-texniki təchizat;
- kabelləşdirmə;
- montaj və instalyasiya;

- sınaq və təlim;
- sistemin administratorluğu (təhlükəsizlik sistemi, məlumat bazaları, kompüter şəbəkəsi, sistemin server, kompüter və proqram təminatı üzrə);
- informasiya-sorğu və xidmətləri;
- informasiya-axtarış və təhlil;
- texniki diaqnostika, təmir-bərpa və utilizasiya;
- kompüter insidentlərinin auditi, təhqiqatı və kiberkriminalistika (sübutların müəyyən edilməsi və toplanması).

**Təhlükəsizlik tələblərinin hədəflər, risklər və əks-vasitələr ilə əlaqəli təsnifatlaşdırılması**

Təhlükəsizlik tələblərinin təsnifatı mümkün riskləri sistemli şəkildə müəyyən etmək, mühafizəni və monitorinqi adekvat olaraq qurmaq üçün əhəmiyyətlidir. İnformasiya sisteminin obyekt, proses və subyektlərinin, bu sistem üçün təhlükəsizlik tələblərinin, bu tələblərlə bağlı olan mümkün risklərin, bu risklərə adekvat olan əks-vasitələrin təsnifatları uzlaşdırıla bilər.

Bu təsnifatlar əsasında müvafiq reyestrlər yaradılıb birləşdirilə bilər. Bunun üçün həmin reyestrlərdə hədəflər və tələblər, tələblər və risklər, risklər və əks-vasitələr arasında səbəb-nəticə üzrə məntiqi əlaqələr identifikasiya edilməli, bu əlaqələr üçün keçid (“link”) nöqtələri göstərilməlidir.

Mümkün risklərə aid təsnifat bölmələri təhlükəsizlik tələblərinə aid təsnifatı və risklərin kateqoriyalarını (hücumlar, zəifliklər), üsullarını (məqsədli hərəkətlər, təsadüf kateqoriyalı hadisələr, texnogen proseslər), mənbələrini (sistemin daxilində olan istifadəçilər, sistemdən kənarda olan obyektlər, texniki gizliclər – “böcək”lər, zərərli təsirə malik fiziki obyektlər, ziyanverici proqramlar – “virus”lar) nəzərə almaqla müəyyən edilə bilər.

İnformasiya sisteminin təhlükəsizliyinin təminat vasitələrinə aid təsnifat mümkün risklərin təsnifatını və bu vasitələrin kateqoriyalarını (təşkilati, proqram-texniki və fiziki) nəzərə almaqla müəyyən edilə bilər.

Təhlükəsizlik hədəflərinə və tələblərinə, risklərə və mühafizə vasitələrinə aid reyestrlər “İnformasiya təhlükəsizliyi siyasəti”nin və normativ qaydaların hazırlanması üçün istifadə edilir.

Bu reyestrlər informasiya sisteminin həyat tsikli proseslərinin, onların iş vahidlərinin (hərəkətlərin, əməliyyatların) icrasını təşkil etmək məqsədilə hazırlanan plan-qrafiklərin informasiya tamlığının təmin edilməsi üçün əhəmiyyətli ola bilər:

- iş vahidləri arasında səbəb-nəticə əlaqələri və şərtlər;
- icra üçün tələb olunan müddət (günlərin sayı);
- icraçı (məsul) şəxs (vəzifə, struktur bölmə, qurum);
- icra üçün lazım olan sənədlər;
- icra üçün istifadə olunan obyektlər (vasitələr);
- icra üçün nəzərə alınan təhlükəsizlik tələbi (tələbləri);
- icraya aid mümkün risklər;
- icra nəticəsində yaranan sənədlər, obyektlər (məhsullar), proseslər (xidmətlər).

Təhlükəsizlik tələblərinin təsnifatlandırılması bu sahəyə nəzarət üçün aşağıdakı mərhələ və proseslərin optimal yaradılması əhəmiyyətlidir:

a) birinci mərhələ – sistemin istismarına başlanılandan əvvəl: ekspertiza; sertifikatlaşdırma; təlim.
b) ikinci mərhələ – sistemin istismarına başlanılandan sonra: monitorinq; attestasiya.

İnformasiya sistemlərinə təhlükəsizlik tələblərinin vahid qaydada təsnifatlaşdırılması bu sahədə monitorinq işlərinin mərkəzləşməsinə imkan yaradır. Bunun üçün monitorinq üzrə təhlükəsizlik parametrləri bu sənəddə göstərilən təhlükəsizlik tələblərinin təsnifatına uyğun seçilməlidir.

Monitorinq üçün aşağıdakı reyestrlərin dayanıqlı işləməsi təmin edilməlidir:

– təhlükəsizlik tələblərinin hədəfi olan obyekt, proses və subyektlərin reyestrləri;

- təhlükəsizlik tələblərinin reyestri;
- informasiya təhlükəsizliyi ilə bağlı mümkün risklərin reyestri;
- mühafizə vasitələrinin reyestri;
- informasiya təhlükəsizliyi insidentlərinin və həllərin reyestri ("biliklər bankı");

Monitorinq hesabatında təhlükəsizlik tələbləri pozulan informasiya sistemləri və aşkar olmuş nöqsanlar təhlükəsizlik tələblərinin təsnifatı üzrə göstərilə bilər. Bu mövcud nöqsanların əhəmiyyətini düzgün qiymətləndirməyə kömək edər.

**Nəticə**

Məlumdur ki, konfidensial məlumatların təhlükəsizliyi onların həyat tsiklinin bütün proseslərində – emal olunduğu informasiya sistemində təmin olunmalıdır. Bunun üçün konfidensial məlumatların hər bir informasiya sisteminə və onun arxitektur obyeklərinə biznes prosesləri və bu proseslərin subyektləri ilə bağlı mümkün risklər müəyyən edilməli, adekvat mühafizə üsulları və vasitələri yaradılıb tətbiq olunmalıdır. Bu məqsədlə məqalədə korporativ informasiya sistemlərində informasiya təhlükəsizliyinin idarə edilməsi üçün informasiya təhlükəsizliyi tələblərinin təsnifat modeli işlənilmişdir. Təhlükəsizlik tələblərinin hədəfləri kimi informasiya sisteminə aid olan obyektlər, proseslər və subyektlər qəbul edilir və onlar üçün təsnifatlar təklif edilir, təsnifat modelinin mümkün riskləri sistemli şəkildə müəyyən etmək, mühafizəni və monitorinqi adekvat olaraq qurmaq üçün əhəmiyyəti qiymətləndirilir. Təhlükəsizlik tələblərinin, bu tələblərlə bağlı olan mümkün risklərin, bu risklərə adekvat olan əks-vasitələrin təsnifatlarının uzlaşdırılması və birləşmiş reyestrin yaradılması üçün zəmin müəyyən edilir.

**Ədəbiyyat**

1. Əliquliyev R.M., İmamverdiyev Y.N., Yusifov F.F., Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar // İnformasiya cəmiyyəti problemləri, 2011, №2, s. 3-9.
2. Əliyev E.A., İnformasiya sistemlərində fərdi məlumatların həyat tsiklinin tənzimlənməsi problemləri // İnformasiya cəmiyyəti problemləri, 2011, №1, s. 56-68.
3. ISO/IEC-27001:2013 Information technology - Security techniques - İnformation security management systems -- Requirements. 2013, 23 p.
4. Colwill C., Human factors in information security: The insider threat - Who can you trust these days? // Information Security Technical Report, 2009, Vol. 14, No. 4, pp. 186-196.
5. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management. 2011, 68 p.

**УДК 004.056**

**Алиев Эльчин А.**
Институт Информационных Технологий НАНА, Баку, Азербайджан
elchinaa@gmail.com

**Модель классификации требований безопасности для управления информационной безопасностью в корпоративных информационных системах**

В этой работе разрабатывается классификационная модель с целью системного определения требований безопасности для управления информационной безопасностью в корпоративных информационных системах. В качестве системообразующих элементов – целей требований безопасности принимаются объекты, процессы и субъекты («человеческий фактор»), принадлежащие к информационной системе, и предлагаются классификационные модели для них. Определяется общая платформа для согласования классификаций требований безопасности, потенциальных рисков, связанных с этими требованиями, и контрмер, адекватных этим рискам, а также создания объединенного реестра.

***Ключевые слова:*** *управление информационной безопасностью, требование безопасности, классификация требований безопасности, цель требований безопасности, адекватная защита, согласование классификаций, объединенный реестр.*

**Elchin A. Aliyev**
Institute of Information Technology of ANAS, Baku, Azerbaijan
elchinaa@gmail.com

**Security requirements classification model for information security management in corporate information systems**

The research paper develops a classification model for the purpose of systematic determination of the information security requirements for information security management in corporate information systems. - processes and subjects ("human factor") belonging to the information system are accepted as model’s system elements - targets of security requirements objects and classification models are proposed for them. The paper defines a common platform for coordination of classifications of security requirements, potential risks associated with these requirements, and adequate counter-measures for these risks, as well as for creating a unified registry.

***Keywords:*** *information security management, security requirements, security requirements classification, security requirement target, adequate protection, coordination of classifications, unified registry.*